PRIVACY IMPACT ASSESSMENT (PIA)

For the

DISA Financial Management Systems
Defense Information Systems Agency

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐ **New DoD Information System**   ☐ **New Electronic Collection**

☒ **Existing DoD Information System**   ☐ **Existing Electronic Collection**

☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒ **Yes, DITPR**   Enter DITPR System Identification Number | 6010

☐ **Yes, SIPRNET**   Enter SIPRNET Identification Number | |

☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ **Yes**   ☒ **No**

If "Yes," enter UPI | |

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is <u>retrieved</u> by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☐ **Yes**   ☒ **No**

If "Yes," enter Privacy Act SORN Identifier | |

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date. | |

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number [   ]

Enter Expiration Date [   ]

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

The authority allows DISA Financial Management Systems to collect the following data:

- DoDD 8500.01E Information Assurance (IA) Certified Current April 23, 2007
- OMB M-99-18, Privacy Policies on Federal Web Sites

---

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The DISA Financial Management System (DFMS) provides DISA with automated support to facilitate Agency financial management and planning. DFMS integrates data from a variety of sources to provide a complete view of the financial evolution of DISA projects. The types of personnel information about DISA individuals collected in the system includes full names, email address, phone number, assigned organization, and other ID (SSOUUID). All of these personnel attributes are stored within an oracle database accessed only be the DFMS application and DFMS developers and administrators. It is not shared with end-user populations.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The PII stored in DFMS is not shared with the general user population and is not available through application front-ends. In particular, the SSN is never shared and remains encrypted while at rest. The Intranet Services userids are stored and passed over an encrypted channel (Secure Socket Layers - SSL) and/or over a trusted private network connection between application, database, and/or directory servers. However, the protected data is not to be shared or displayed outside of back-end system functions. The risks associated with the storage of the PII within Intranet Services are minimal due to the defense-in-depth strategy employed by Department of Defense, DISA, and the developers and system administrators of Intranet Services and DFMS.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☐ **Within the DoD Component.**

    Specify. [ ]

☒ **Other DoD Components.**

    Specify. [Defense Finance and Accounting Service (DFAS)]

☐ **Other Federal Agencies.**

    Specify. [ ]

☐ **State and Local Agencies.**

    Specify. [ ]

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

    Specify. [ ]

☐ **Other** (e.g., commercial providers, colleges).

    Specify. [ ]

i. Do individuals have the opportunity to object to the collection of their PII?

☐ Yes   ☒ No

    (1) If "Yes," describe method by which individuals can object to the collection of PII.

    (2) If "No," state the reason why individuals cannot object.

The PII information is not collected at run-time, meaning that the user of the system does not need to directly provide PII to DFMS at any time before, during, or after their session. PII information is "known" to the system because of the backend system integration with the DISA authoritative source for these personnel identity attributes.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ Yes   ☒ No

    (1) If "Yes," describe the method by which individuals can give or withhold their consent.

    (2) If "No," state the reason why individuals cannot give or withhold their consent.

Their consent is inherent to providing secure access to DISA information and services based on who they are within the organization. Consent is implied as an employee of DISA.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐   **Privacy Act Statement**   ☐   **Privacy Advisory**

☐   **Other**   ☒   **None**

Describe each applicable format.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.